



IPS Engine - Release Notes

Version 6.4

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



June 15, 2021

IPS Engine 6.4 Release Notes

43-640-698431-20210615

TABLE OF CONTENTS

Change log	4
Introduction	5
Product integration and support	6
Resolved issues	7
Known issues	9

Change log

Date	Change Description
2021-06-15	Initial release.

Introduction

This document provides the following information for the Fortinet IPS Engine 6.4 build 091.

- [Product integration and support on page 6](#)
- [Resolved issues on page 7](#)
- [Known issues on page 9](#)

IPS Engine 6.4 build 091 is a built-in release for FortiOS 6.4.6. It is not a release to FortiGuard.

For additional FortiOS documentation, see the [Fortinet Document Library](#).

Product integration and support

The following table lists IPS engine product integration and support information:

FortiOS	6.4.6
---------	-------

Resolved issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquiries about a particular bug, contact [Customer Service & Support](#).

Bug ID	Description
580391	Unable to create MAC address-based policies in NGFW.
654356	Under NGFW policy mode, sessions are not revalidated when security policies change. A work around is to clear session after policy change.
662698	One-arm sniffer logging shows inaccurate SNMP application sent bytes.
672994	Web filter warning message does not contain certification chain.
676705	Custom IEC-104 app-ctrl signatures skipped after signature database update.
677834	HTTP traffic is dropped when custom proxy options are applied to policy.
681611	IPS engine crashes with 5.218 ips_dlp_alert.
683669	Firewall schedule settings do not follow daylight savings time.
688888	bzip2 including eicar is detected in the original direction of the flow mode firewall policy even though scan-bzip2 is disabled.
691196	One arm IPS URL filter cannot block HTTPS websites.
695441	Not able to get past block/override or warning page when doing a web filter override in flow mode.
695774	Remote category flow and proxy mode wildcard matching difference.
696619	FGSP-synced UDP sessions may be blocked in NGFW policy mode when asymmetric routing is used due to policy matching failure. Other types of traffic may also be affected (e.g. TCP) in the case of failover of the reply-direction traffic to a different FortiGate in the FGSP cluster.
696753	Chassis multiple IPS crashes and UTM web filter impact after enabling web filter content-header.
696819	IPS Engine archive timestamp dated from 1970.
707907	IPS Engine in flow deep inspection does not decrypt some TLS 1.3 session and causes problem with application control detection.
713068	FGSP support in NGFW policy mode.
715136	High memory usage for some slab objects.
718452	<code>set https-replacemsg disable</code> causes connection RST on URLs in URL filter list in flow inspection.
719007	URL filtering followed by /* causes rating error.

Bug ID	Description
719252	IPS Engine crashes.
721462	Memory usage increases to conserve mode after IPS Engine upgrade.

Known issues

There are no known issues with this release of IPS engine version 6.4 for FortiOS.

To report a bug, please contact [Customer Service & Support](#).



FORTINET®



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.